DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

26 JAN 2016

SAIS-CB

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Privileged/Elevated Access to Army Information Systems, Networks and Data

1. References.

a. Army Regulation (AR) 25-2, Information Assurance (IA), 23 March 2009.

b. AR 25-1, Army Information Technology (IT), 25 June 2013.

c. Department of Defense (DoD) 8570.01-M, IA Workforce Improvement Program, 24 January 2012.

d. Memorandum, Chief Information Officer/G-6, 11 August 2014, subject: Privileged Access to Army Information Systems and Networks.

e. Department of Defense Directive (DoDD) 8140.01, Cyberspace Workforce Management, 11 August 2015.

2. Effective immediately, this memorandum rescinds reference d and provides updated and supplemental guidance.

3. Purpose. This memorandum establishes policy and responsibilities regarding privileged users. As part of the policy, Commands will continue to direct actions associated with the request for, receipt of and monitoring of Soldiers, civilians, contractors, vendors and any other individuals with privileged access to Army information systems, networks and data (i.e., users with elevated privileges, also known as privileged users).

4. Applicability. This policy applies to the active Army, the Army National Guard / Army National Guard of the United States and the U.S. Army Reserve.

5. Policy.

a. Commands and other Army activity commanders and managers will nominate

Soldiers, civilians, contractors and other individuals as candidates for privileged/elevated access via signed (physical or digital) appointing letters to their respective service provider. Privileged users are individuals who are authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Commands and other Army activity managers must in the appointment letters:

(1) Designate the information technology (IT) personnel security standard based upon the sensitivity of functions performed by individuals with certain privileges, in accordance with AR 25-2.

(2) Designate the cybersecurity workforce category/specialty/work role per DoD 8570.01-M and the DoD Cyberspace Workforce Framework (DCWF) (under DoDD 8140.01).

(3) Specify the functions to be performed by the candidate that require privileged/elevated access.

(a) Functions must be specified at the unclassified level and should not contain specific server names, IP addresses or other potentially sensitive information.

(b) Enter critical functions, per the DCWF knowledge skill abilities (KSA) and/or functions in reference c, to establish that privileged/elevated access is necessary to perform the function.

(c) Identify each function as "above baseline", or one of the following delivered IT support services, per AR 25-1 (reference b): "baseline," "enhanced," "mission-funded" or "mission-unique." This can be determined by the Network Enterprise Center (NEC), IT service provider or funding source for the position/services. (An example of function specification: "Mission-funded: Full privileged access required on non-enterprise servers of the 36th Infantry Division in order to install operating system and software patches, and to conduct backups.")

b. Each candidate for privileged/elevated access must complete and sign (physical or digital) a privileged access agreement (PAA) and a non-disclosure agreement (NDA). The PAA and NDA may be combined into a single document. The PAA must be signed by the Command's/organization's Information System Security Manager (ISSM) or Information System Security Officer (ISSO) who oversees network security.

c. Templates for the appointment letter, PAAs and NDAs are available in the Documents section of the Army Training & Certification Tracking System (ATCTS), located at https://atc.us.army.mil. Commands and other Army activities may expand

upon the content in the templates.

d. Commands and other Army activities must upload completed/signed appointment letters, PAAs and NDAs into the individual's ATCTS profile.

e. For enterprise managed system user accounts, NECs or designated service providers will authorize and deny the granting of privileged/elevated access. For Command/organization user accounts, the appointed ISSM or ISSO who oversees the cybersecurity/information assurance security program will deny or authorize the request for granting of privileged access before forwarding to the NEC or service provider for consideration.

(1) Requests for user privileged/elevated access will be made via DD Form 2875, System Authorization Access Request.

(2) Authorization and denial decisions will be documented on DD Form 2875, System Authorization Access Request, block 13 (Justification for Access), and uploaded to the individual's Army Training and Certification Tracking System profile. Additionally, the DD 2875 will be sent to the requesting Command or other Army activity, giving it the opportunity to resubmit the request.

(3) Disagreements regarding enterprise and provider-managed user accounts will be escalated to the director of the NEC/service provider. For other user accounts, disagreements will be escalated to the appointed ISSM/ISSO.

(4) The final arbiter of any disagreement concerning authorization or denial of privileged/elevated access will be the appointed authorizing official/designated approving authority (AO/DAA) of the Army Signal Command (Theater) or other area of responsibility.

f. The specific NECs or designated service providers responsible for authorizing, denying and managing users' privileged/elevated access, when not clear and agreed upon, will be determined by the Theater Signal Commander.

6. Directed actions.

a. Commanders, program managers, Theater Signal Commands, Signal Brigades, NECs, designated service providers and cybersecurity/information assurance personnel will ensure enforcement of this policy.

b. Commands and other Army activities with users who have privileged/elevated access will promptly, upon signing of this memorandum:

(1) Revalidate all users with privileged/elevated access, and thereafter on a quarterly basis, to ensure that such access is commensurate with: current mission requirements; the user's position/work role; a need for the user to perform functions that specifically require privileged/elevated access; and reassessment of least privilege and separation of duties. Commands/activities must ensure that role assignments are distinct, and must minimize roles and role assignments that allow root access. Quarterly reviews will be completed and verified in ATCTS. This feature is currently available for all ATCTS managers.

(2) Coordinate with their NECs and IT service providers to oversee this policy and its associated process via quarterly reviews of documentation (e.g., appointment letters, PAAs, NDAs, decisions) for the request, authorization and denial of privileged/elevated access.

(3) Incorporate procedures to promptly revoke privileged/elevated access from any user account as soon as the user position and/or function no longer requires such access.

(a) Prior to departure, disable privileged/elevated user accounts for all individuals who are no longer employed, have been reassigned or will be on extended absence.

(b) Reduce overlapping functions and privileges, as appropriate, to meet mission needs.

(c) Promptly notify and coordinate with the respective NEC, IT service provider or ISSM/ISSO to accomplish user account changes.

(d) Promptly notify and coordinate with security managers to ensure continuity of required suitability investigations and contract security requirements, in accordance with the IT standards and any classification or caveats.

(4) Ensure that all privileged/elevated users log into their ATCTS account and choose a work role in the profile's "position" field. This will enable privileged users to start aligning with the work role designations required by reference c, chapter 9.

(5) Remove or update the appointment letter in ATCTS when privileged/elevated access has been denied or is no longer required. The PAA must be removed as well.

(6) Ensure that all individuals with privileged/elevated access have completed and signed (physically or digitally) an appointment letter, PAA and NDA, which shall be uploaded to ATCTS.

c. NECs, designated service providers and ISSMs/ISSOs will:

(1) Revoke privileged/elevated access for user accounts whose documentation is not fully compliant. Provide notice of this revocation to the individual holding the user account and his/her associated Command or other Army activity.

(2) Ensure that all individuals with privileged/elevated access have completed and signed (physically or digitally) an appointment letter, PAA and NDA before granting access.

(3) Promptly revoke user account privileged/elevated access upon notification from the Command or other Army activity that such access is no longer required.

d. Army Cyber Command and Second Army will, in accordance with General Order 2014-02, develop and publish Army-wide orders and procedures for privileged/elevated access in accordance with Army, DoD and national policies; update these documents as needed; and publish these documents on both the NIPRNet and SIPRNet.

7. This policy will remain in effect until incorporated into AR 25-2.

8. The Chief Information Officer/G-6 points of contact for this memorandum are: Ms. Melissa Hicks, melissa.c.hicks.civ@mail.mil or (703) 545-1604; and Ms. Phyllis Bailey, Phyllis.e.bailey2.civ@mail.mil or (703) 545-1698.

Digitally signed by FERRELL.ROBERT.SILAS.1028607268
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=FERRELL.ROBERT.SILAS.1028607268
Date: 2016.01.26 13:36:22 -05'00'

ROBERT S. FERRELL
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
Principal Officials of Headquarters, Department Of The Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Pacific
U.S. Army Europe
U.S. Army Central
U.S. Army North
(CONT)

DISTRIBUTION: (CONT)
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade
Commandant, U.S. Army War College
Commander, Second Army

CF:
Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army
Commander, U.S. Army Cyber Command